FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards
and Technology of the United States
of America

The Communications Security
Establishment of the Government
of Canada

Consolidated Certificate No. 0052

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael J Cooper
Dated: 4 May 2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:
Dated: 4 May 2015

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2344	04/08/2015	Dell W-620 and W-650 Mobility Controllers with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-620-F1, W-620-USF1, W-650-F1 and W-650-USF1 with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS
2345	04/08/2015	Dell W-AP134 and W-AP135 Wireless Access Points with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-AP134-F1 and W-AP135-F1 with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS
2346	04/08/2015	Dell W-IAP3WN, W-IAP3WNP, W-IAP108, W-IAP109, W-AP114, and W-AP115 Wireless Access Points with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-IAP3WN-F1, W-IAP3WN-USF1, W-IAP3WNP-F1, W-IAP3WNP-USF1, W-IAP108-F1, W-IAP108-USF1, W-IAP109-F1, W-IAP109-USF1, W-AP114-F1 and W-AP115-F1 with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS
2347	4/15/2015	Dell W-3000 and W-6000/M3 Mobility Controllers with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-3200-F1, W-3200-USF1, W-3400-F1, W-3400-USF1, W-3600-F1, W-3600-USF1 and [(W-6000-F1 or W-6000-USF1) with W-6000M3, and (HW-PSU-200 or HW-PSU-400)] with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS
2348	04/17/2015	HGST Ultrastar He8 TCG Enterprise HDDs	HGST, Inc.	Hardware Versions: HUH728080AL5205 (0001), HUH728060AL5205 (0001), HUH728080AL4205 (0001) and HUH728060AL4205 (0001); Firmware Version: R515
2350	04/20/2015	Canon MFP Security Chip	Canon Inc.	Hardware Versions: FK4-1731A, FK4-1731B; Firmware Version: 2.10

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2352	04/10/2015	BitLocker® Windows OS Loader (winload) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17031
2353	04/23/2015	BitLocker® Windows Resume (winresume) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 2, Surface Pro, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17031
2354	04/23/2015	BitLocker® Dump Filter (dumpfve.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 2, Surface Pro,Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17031
2355	04/17/2015	Code Integrity (ci.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17031

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2357	04/30/2015	Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17031
2358	04/13/2015	Astro Subscriber Motorola Advanced Crypto Engine (MACE)	Motorola Solutions, Inc.	Hardware Versions: P/Ns 5185912Y01, 5185912Y03 and 5185912Y05; Firmware Versions: R01.05.12 and [R01.00.00 or (R01.00.00 and R02.00.00)]
2359	04/13/2015	IronKey H350	Imation Corp.	Hardware Versions: P/Ns MXKB1B500G5001FIPS and MXKB1B001T5001FIPS; Firmware Version: 1.0.0
2360	04/13/2015	IPCryptR2	Motorola Solutions, Inc.	Hardware Version: BLN1306A; Firmware Version: R06.01.00
2361	04/23/2015	SSL Visibility Appliance	Blue Coat® Systems, Inc.	Hardware Versions: SV3800; 090-03064 and 080-03563 with FIPS Kit: FIPS-LABELS-SV; Firmware Version: 3.8.2F build 227
2362	04/23/2015	SSL Visibility Appliance	Blue Coat® Systems, Inc.	Hardware Versions: SV1800-C [1], SV1800-F [2] and SV2800 [3]; 090-03061 [1], 080-03560 [1], 090-03062 [2], 080-03561 [2], 090-03063 [3] and 080-03562 [3] with FIPS Kit: FIPS-LABELS-SV; Firmware Version: 3.8.2F build 227
2363	04/27/2015	Cisco Systems 5760 Wireless LAN Controller	Cisco Systems, Inc.	Hardware Version: Cisco Systems 5760 Wireless LAN Controller; Firmware Version: IOS XE 03.06.00aE

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2364	04/28/2015	Dell OpenSSL Cryptographic	Dell, Inc.	Software Version: 2.1